IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A method for summarizing firewall activity, comprising:

(a) organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;

(b) tracking a number of occurrences of each type of event utilizing the firewall; and

(c) displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;

wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;

wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:

upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

2. (Original) The method as recited in claim 1, wherein the events include blocked attempts of various types.

3. (Currently Amended) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts of the remote computers to access predetermined banned ports associated with the local computer.

4. (Currently Amended) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts of the remote computers with a predetermined set of ~~Internet Protocol (~~IP~~)~~ addresses to access the local computer.

5. (Currently Amended) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts to access ~~a~~the network made by predetermined applications.

6. (Currently Amended) The method as recited in claim 1, wherein the displayed number of occurrences of each type of event occurred within a predetermined time period.

7. (Currently Amended) The method as recited in claim 1, and further comprising displaying additional information relating to the events upon ~~the~~ selection thereof.

8. (Currently Amended) The method as recited in claim 2, wherein a first type of the blocked attempts includes blocked attempts of the remote computers to

access predetermined banned ports associated with the local computer, a second type of the blocked attempts includes blocked attempts of the remote computers with a predetermined set of ~~Internet Protocol~~ (IP) addresses to access the local computer, and a third type of the blocked attempts includes blocked attempts to access athe network made by predetermined applications.

9. (Currently Amended) The method as recited in claim 8, wherein the first type of the blocked attempts, the second type of the blocked attempts, and the third type of the blocked attempts are organized into the categories.

10. (Original) The method as recited in claim 8, wherein a plurality of banned ports associated with the first type of the blocked attempts are displayed with the number of the occurrences associated therewith.

11. (Original) The method as recited in claim 8, wherein a plurality of banned IP addresses associated with the second type of the blocked attempts are displayed with the number of the occurrences associated therewith.

12. (Original) The method as recited in claim 8, wherein a plurality of banned applications associated with the third type of the blocked attempts are displayed with the number of the occurrences associated therewith.

13. - 18. (Cancelled)

19. (Currently Amended) A computer program product embodied on a computer readable medium for summarizing firewall activity, comprising:

(a) computer code for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;

(b) computer code for tracking a number of occurrences of each type of event utilizing the firewall; and

(c) computer code for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;

wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;

wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:

upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

20. (Currently Amended) A system for summarizing firewall activity, comprising:

(a) logic for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;

(b) logic for tracking a number of occurrences of each type of event utilizing the firewall; and

(c) logic for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;

wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;

wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:

upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

21 (Currently Amended) A system for summarizing firewall activity, comprising:

(a) means for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;

(b) means for tracking a number of occurrences of each type of event utilizing the firewall; and

(c) means for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;

wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;

wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:

upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

22. – 23. (Cancelled)

24. (Currently Amended) A firewall method, comprising:

(a) executing a firewall in association with a local computer;

(b) identifying a number of blocked attempts of remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer;

(c) identifying a number of attempts of the remote computers to access predetermined frequently-used ports associated with the local computer;

(d) identifying a number of blocked attempts to access a network made by predetermined applications on the local computer;

(e) displaying a menu for selecting from a plurality of interface features including a summary page, an applications page, an event log, and an IP address page;

(f) upon the selection of the summary page on the menu,

(i) displaying a recent activity list including recent activity icons corresponding to events including total blocked attempts, the attempts of the remote computers to access the predetermined frequently-used ports associated with the local computer, the blocked attempts of the remote computers with the predetermined set of IP addresses to access the local computer, the recent activity list further including a total number of the events within a predetermined time period corresponding with each recent activity icon, and a graphical representation indicating a severity of the total number of the events,

(ii) displaying a frequently accessed port list including port icons corresponding to the predetermined frequently-used ports, the frequently accessed port list further including a total number of the attempts corresponding with each predetermined frequently-used ports, and a graphical representation indicating a severity of the total number of the attempts,

(iii) displaying a commonly blocked IP address list including IP address icons corresponding to banned IP addresses from which the blocked attempts of the remote computers occurred, the commonly blocked IP

address list further including a total number of the blocked attempts corresponding with each IP address icon, and a graphical representation indicating a severity of the total number of the blocked attempts,

(iv) displaying a commonly blocked application list including application icons corresponding to banned applications associated with the blocked attempts, the commonly blocked application list further including a total number of the blocked attempts corresponding with each application icon, and a graphical representation indicating a severity of the total number of the blocked attempts;

(g) upon the selection of the applications page on the menu, displaying an applications interface for selecting the predetermined applications;

(h) upon the selection of the untrusted IP address page on the menu, displaying an untrusted IP address interface for selecting the IP addresses associated with remote computers to be blocked; and

(i) upon the selection of the event log on the menu, displaying a log of the attempts;

wherein a slider bar is displayed for setting a blocking level of the firewall by sliding the slider bar to a desired blocking level;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over the network.

25. – 26. (Cancelled)